Firepowerデバイスでのエレファントフローの検出

内容

はじめに

このドキュメントでは、Cisco Firepower Threat Defense(FTD)環境でエレファントフロー検出(FFT)を実行する方法について説明します。

前提条件

要件

次の製品に関する知識があることが推奨されます。

- Firepower Management Center（FMC）
- Firepower Threat Defense（FTD）
- NetFlow

使用するコンポーネント

このドキュメントの情報は、ソフトウェアバージョン7.1以降を実行するFMCに基づくものです。 このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメント内で使用されているデバイスはすべて、クリアな設定（デフォルト）から作業を始めています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco Firepowerのエレファントフロー検出は、大量のネットワークリソースを消費してパフォー

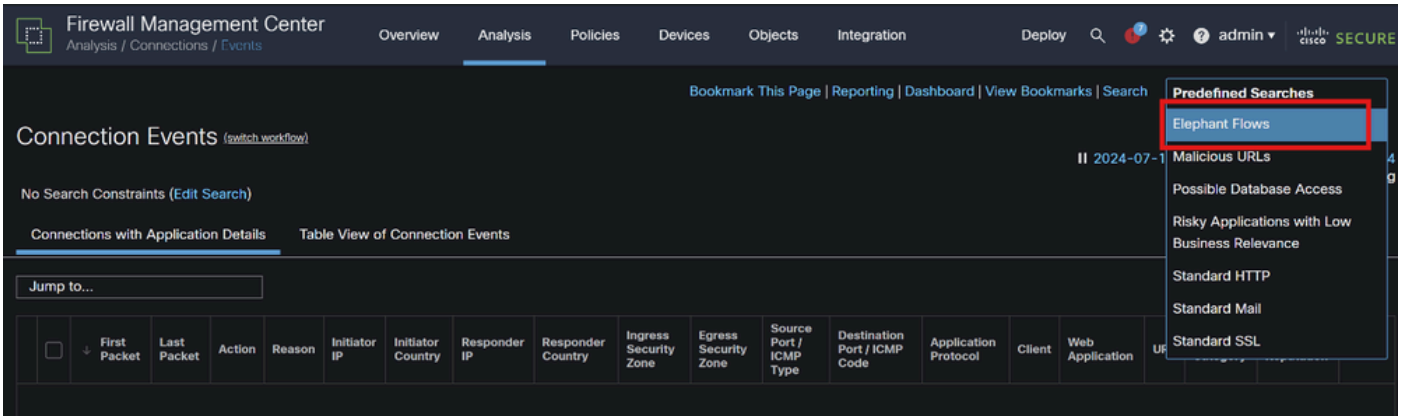
マンスに影響を与える可能性がある、長期間使用される大規模なフローを特定して管理するために不可欠です。エレファントフローは、ビデオストリーミング、大きなファイルの転送、データベースレプリケーションなど、データ量の多いアプリケーションで発生する可能性があります。これは、次の方法を使用して識別できます。

方式

1. FMCの使用

エレファントフロー検出は、リリース7.1で導入されました。リリース7.2では、カスタマイズが容易になり、エレファントフローをバイパスまたは抑制するオプションが提供されます。Snort 3デバイスでは、インテリジェントアプリケーションバイパス(IAB)はバージョン7.2.0以降では廃止されています。

エレファントフローの検出は、Analysis > Connections > Events > Predefined Searches > Elephant Flowsで実行できます。



接続イベント

このドキュメントでは、アクセスコントロールポリシーでエレファントフローを設定するための手順について説明します

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72/elephant-flow.html#task_sxp_h2d_jsb

2. CLIの使用

a. SnortインスタンスのCPUスパイクは、ネットワークがエレファントフローを処理していることを示す場合もあります。エレファントフローは次のコマンドで特定できます。

show asp inspect-dp snort (隠しコマンド)

コマンド出力の例を次に示します。

> show asp inspect-dp snort (隠しコマンド)

SNORTインスペクションインスタンスステータス情報ID PID

Cpu-Usage Conns Segs/Pkts Status Tot(usr | sys)

— ----- ---------- ---------- ---------- ----------

0 16450 8% (7%| 0 %) 2.2 K 0対応

1 16453 9% (8%| 0 %) 2.2 K 0対応

2 16451 6% (5%| 1 %) 2.3 K 0対応

3 16454 5% (5%| 0 %) 2.2 K 1対応

4 16456 6% (6%| 0 %) 2.3 K 0対応

5 16457 6% (6%| 0 %) 2.3 K 0対応

6 16458 6% (5%| 0 %) 2.2 K 1対応

7 16459 4% (4%| 0 %) 2.3 K 0対応

8 16452 9% (8%| 1 %) 2.2 K 0対応

9 16455 100% (100%| 0%) 2.2 K 5 READY <<<<高いCPU使用率

10 16460 7% (6%| 0 %) 2.2 K 0対応

— ----- ---------- ---------- ---------- ----------

概要15% (14%| 0%) 24.6 K 7

b.また、ルートモードからのコマンド出力の「top」は、Snortインスタンスが稼働しているかどうかを確認する際にも役立ちます。

c.このコマンドを使用して接続の詳細をエクスポートし、ファイアウォールを通過するトップトラフィックを確認します。

show asp inspect-dp snort (隠しコマンド)

show connの詳細 | リダイレクトdisk0:/con-detail.txt

このファイルはLinuxモードの「/mnt/disk0」の下にあります。**/ngfw/var/common**に同じものをコピーして、FMCからダウンロードします。

エキスパートcp

/mnt/disk0/<ファイル名> /ngfw/var/common/

次に、接続の詳細な出力例を示します。

UDP内部：10.x.x.x/137内部：10.x.x.43/137、flags - N1、idle 0s、**uptime 6D2h**、timeout 2m0s、**bytes 123131166926** << 123 GBで、稼働時間は6日2時間と見えます

接続参照キーID: 2255619827

UDP内部：10.x.x.255/137内部：10.x.x.42/137、フラグ – N1、アイドル状態0、稼働時間7D5h、タイムアウト2m0s、バイト116338988274

接続参照キーID: 1522768243

UDP内部：10.x.x.255/137内部：10.x.x.39/137、flags - N1、idle 0s、uptime 8D1h、timeout 2m0s、bytes 60930791876

接続参照キーID: 1208773687

UDP内部：10.x.x.255/137内部：10.x.x0.34/137、flags - N1、idle 0s、uptime 9D5h、timeout 2m0s、bytes 59310023420

接続参照キーID: 597774515

3. Netflowの使用

エレファントフローは、ネットワークのパフォーマンスに影響を与える可能性がある大量のトラフィックフローです。これらのフローを検出するには、ネットワークトラフィックを監視して、大規模で永続的なフローを示すパターンを特定する必要があります。Cisco Firepowerは、エレファントフローを含むネットワークトラフィックを検出および分析するツールと機能を提供します。NetFlowツールは、モニタリング用のIPトラフィック情報の収集に役立ちます。

このドキュメントでは、FMCでNetFlowポリシーを設定するための手順について説明します

https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-management-center-virtual/221612-htz-01-2024-configure-netflow-in-fmc.html

収集したデータを分析するには、NetFlowコレクタとアナライザ（Cisco Stealthwatch、SolarWinds、その他のNetFlow分析ツールなど）を使用します。ゾウの流れを特定したら、その影響を軽減するための対策を講じることができます。

- トラフィックシェーピングとQoS:Quality of Service(QoS)ポリシーを実装して、トラフィックに優先順位を付け、エレファントフローの帯域幅を制限します。
- アクセスコントロールポリシー：エレファントフローを管理および制限するアクセスコントロールポリシーを作成します。
- セグメンテーション：ネットワークのセグメンテーションを使用して、大量のフローを分離し、ネットワークの他の部分への影響を最小限に抑えます。
- ロードバランシング：ロードバランシングを実装して、ネットワークリソース間でトラフィックをより均等に分散させます。

4. 継続的なモニタリングと調整

ネットワークトラフィックを定期的に監視して新しいエレファントフローを検出し、必要に応じてポリシーと設定を調整します。

このプロセスを使用すると、Cisco Firepower導入環境のエレファントフローを効果的に検出および管理でき、ネットワークのパフォーマンスとリソースの使用率を向上させることができます。

関連情報

Cisco Secure Firewall Management Centerデバイス設定ガイド、7.2

FMCでのNetFlowの設定

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。